PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-127905
(43)Date of publication of application : 09.05.2000

(51)Int.Cl. B60R 25/10
B60R 25/04
E05B 49/00
E05B 65/12

(21)Application number : 11-291935
(22)Date of filing : 14.10.1999

(71)Applicant : ALCATEL
(72)Inventor : WEIK HARTMUT

(30)Priority
Priority number : 98 19848001 Priority date : 17.10.1998 Priority country : DE

(54) OPERABLY RELEASING METHOD FOR AUTOMOBILE, AND CHIP CARD AND VEHICLE DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for preventing an automobile user who has only a chip card from operating an automobile easily without permission.
SOLUTION: A data carrier stores user intrinsic information about an owner. The information is detected by a reader, supplied into an onboard processor and compared with that stored therein. Further personal information is required of a user by an onboard identification device, supplied into the processor and compared with that about a permissible user identify stored in the onboard. According to results of the comparison of the personal data, an automobile is released to be operable. Thus, the automobile can be hardly used without permission even in the case of using a 'correct' chip card.

LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－127905
（P2000－127905A）
(43)公開日　平成12年５月９日(2000.5.9)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
B60R 25/10	615	B60R 25/10	615	
	604		604	
	618		618	
	619		619	
25/04	606	25/04	606	

審査請求　未請求　請求項の数27　ＯＬ　外国語出願　（全 22 頁）　最終頁に続く

(21)出願番号　特願平11－291935
(22)出願日　平成11年10月14日(1999.10.14)
(31)優先権主張番号　19848001．6
(32)優先日　平成10年10月17日(1998.10.17)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　391030332
アルカテル
フランス国、75008　パリ、リュ・ラ・ボエティ　54
(72)発明者　ハルトムート・バイク
ドイツ国、70195・シュトウツトガルト、フンメルベルクシュトラーセ・15
(74)代理人　100062007
弁理士　川口　義雄　（外２名）

(54)【発明の名称】　自動車両を動作可能に解除する方法およびそのためのチップカードおよび車両装置

(57)【要約】
【課題】　無許可の自動車両ユーザが、チップカードを保有しているだけは簡単に自動車両を動作可能に解除できない方法を提供する。
【解決手段】　データキャリアは所有者に関するユーザ固有の情報を記憶しており、その情報はリーダによって検出され、オンボードプロセッサに供給され、そこに記憶されている情報と比較され、さらなる個人情報がオンボード認識装置によってユーザに要求され、プロセッサに供給され、許可できるユーザのアイデンティティに関するオンボードで記憶されている情報と比較され、個人データの比較の結果に応じて、自動車両が動作可能に解除されることを特徴とする。このようにすると、「正しい」チップカードが利用できる場合でも自動車両の無許可の使用をほとんどなくすことが可能になる。

【特許請求の範囲】

【請求項１】　たとえばイグニションシステムおよび／または燃料供給を解除し、かつ／または自動車両の警報システムを働かないようにすることによって自動車両を動作可能に解除する方法であって、データキャリア、特にチップカードをオンボードリーダに供給した結果、供給されたデータキャリアが有効であり、解除を許可するデータが記憶されていることをリーダが認識したときに、動作可能に解除することが行われる方法であり、データキャリアにはデータキャリアの所有者に関するユーザ固有の情報が記憶され、その情報はリーダによって検出されてオンボードプロセッサに供給され、そこでオンボードで記憶されている情報と比較されること、また比較の結果に応じて、さらなる個人情報がオンボード認識装置によってユーザに要求され、オンボードプロセッサに供給され、許可できるユーザのアイデンティティに関するオンボードで記憶されている情報と比較されること、また個人データの比較の結果に応じて、自動車両を動作可能に解除することが行われたり、行われないことを特徴とする方法。

【請求項２】　個人情報が、英数字コードの形式、特に、一般に許可されたユーザにのみ知られている暗証番号（個人識別番号＝ＰＩＮ）の形式で認識装置に入力されることを特徴とする請求項１に記載の方法。

【請求項３】　個人情報が、ユーザの電子指紋の形式で認識装置に供給されることを特徴とする請求項１または２に記載の方法。

【請求項４】　個人情報が、音響信号によって認識装置に供給されることを特徴とする請求項１から３のいずれか一項に記載の方法。

【請求項５】　オンボード音声認識装置によって認識され、動作可能に解除することを許可する記憶されているコードワードと比較されるコードを、音響信号が含むことを特徴とする請求項４に記載の方法。

【請求項６】　音響信号が、ユーザの発した音声信号を含み、オンボード音声認識装置中で、動作可能に解除することを許可する特定のユーザの音声の記憶されている周波数パターンと比較されることを特徴とする請求項４または５に記載の方法。

【請求項７】　個人情報が、光信号の形式で認識装置に供給されることを特徴とする請求項１から６のいずれか一項に記載の方法。

【請求項８】　光信号が、特定の周波数の光および／またはパルス列の光を含んでおり、動作可能に解除することを許可する記憶されている周波数および／またはパルス列とオンボードで比較されることを特徴とする請求項７に記載の方法。

【請求項９】　光信号が、イメージパターンを含んでおり、オンボードイメージ認識装置中で、動作可能に解除することを許可する記憶されているイメージパターンと比較されることを特徴とする請求項７または８に記載の方法。

【請求項１０】　イメージパターンが特定のユーザの顔を含んでいることを特徴とする請求項９に記載の方法。

【請求項１１】　個人情報が、特定のユーザの体重信号によって認識装置に供給され、体重信号が、許可されたユーザのオンボードで記憶されている重量値と比較されることを特徴とする請求項１から１０のいずれか一項に記載の方法。

【請求項１２】　許可できるユーザのアイデンティティに関するオンボードで記憶されている情報を、マスタコードにより変更できることを特徴とする請求項１から１１のいずれか一項に記載の方法。

【請求項１３】　好ましくは特定のユーザが追加のコマンドを入力する結果、オンボードプロセッサが少なくとも１つの個人電子日誌を付けることを特徴とする請求項１から１２のいずれか一項に記載の方法。

【請求項１４】　マスタコードが知られている場合でも後で操作できないように、電子日誌のデータが書込み保護付きでオンボードで記憶されることを特徴とする請求項１３に記載の方法。

【請求項１５】　データキャリア上に記憶されたユーザ固有の情報が、所有者に関する公式データ、特に所有者の運転免許に関するデータを含んでいることを特徴とする請求項１から１４のいずれか一項に記載の方法。

【請求項１６】　データキャリア上に記憶されたユーザ固有の情報が、保険会社のデータ、特に所有者の第三者保険に関するデータを含んでいることを特徴とする請求項１から１５のいずれか一項に記載の方法。

【請求項１７】　データキャリア上に記憶されたユーザ固有の情報が、金融機関のデータ、特に所有者の勘定残高や信用等級に関するデータを含んでいることを特徴とする請求項１から１６のいずれか一項に記載の方法。

【請求項１８】　特定の機関の許可された代理人のみが、所有者のデータキャリア上で、公式データ、保険会社データ、金融機関データを入力または変更するできることを特徴とする請求項１５から１７のいずれか一項に記載の方法。

【請求項１９】　特定の機関の適当な装置によって、所有者のデータキャリア上で、公式データ、保険会社データ、金融機関データが自動的に変更されることを特徴とする請求項１８に記載の方法。

【請求項２０】　ユーザのデータキャリアおよび／またはオンボード認識装置によって供給された情報のオンボードでの評価が、特に無線によってデータバンク問合せを行うことによって実行されることを特徴とする請求項１から１９のいずれか一項に記載の方法。

【請求項２１】　解除された自動車両の運転者を識別するユーザ固有の情報の少なくとも一部が、外部装置、たとえば警察の速度検査地点、国境管理地点、駐車場また

はホテルまたは修理工場へのアクセス装置、現金自動預入支払装置などへ、たとえば無線によって転送されることを特徴とする請求項１から２０のいずれか一項に記載の方法。

【請求項２２】　ユーザ固有の情報が、特定のユーザの個人化されたプリセットパラメータに従って、座席、ステアリングホイール、ミラーなどの自動車両要素を個別に調整するために使用されることを特徴とする請求項１から２１のいずれか一項に記載の方法。

【請求項２３】　認識装置またはプロセッサ中での個人データ比較結果が連続して数回否定的であった場合、警報が発せられることを特徴とする請求項１から２２のいずれか一項に記載の方法。

【請求項２４】　請求項１から２３による１つまたは複数の方法の方法ステップを実行するために、ユーザ固有の情報を含んでいる記憶手段を備えた自動車両を動作可能に解除するデータキャリア、特にチップカード。

【請求項２５】　請求項１から２３による１つまたは複数の方法の方法ステップを実行するための手段を備えた車両装置。

【請求項２６】　ユーザのデータキャリアからユーザ固有の情報を検出するリーダが、さらなる個人情報を要求するためのオンボード認識装置を含んでいることを特徴とする請求項２５に記載の車両装置。

【請求項２７】　オンボードプロセッサが、無線インタフェースを介して外部データ処理システムに接続されることを特徴とする請求項２５または２６に記載の車両装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、たとえばイグニションシステムおよび／または燃料供給を解除し、かつ／または自動車両の警報システムを働かないようにすることにより、自動車両を動作可能に解除する方法であって、データキャリア、特にチップカードをオンボードリーダに供給した結果、供給されたデータキャリアが有効であり、解除を許可するデータが記憶されていることをリーダが認識したときに、動作可能に解除が行われる方法に関し、また本発明は、そのための適当なデータキャリアおよび対応する車両装置に関する。

【０００２】

【従来の技術】このような方法は、ＳＥ　９３００３２９Ａから知られている。

【０００３】自動車両の無許可の使用、特に盗難を防止するための技術的な装置が、いくつか市販されている。自動車両の生産が始まって以来利用されてきたロック可能な自動車両のドアの他に、数１０年もの間、通常は同時に自動車両のドアも開くイグニションキーを使って一般的に解除できるイグニションロックが使用されてきた。

【０００４】このような機械式ロックは、技術的なノウハウを持つ泥棒であれば容易に「破る」ことができるため、盗難増大に対応して電子チップ内蔵の盗難防止磁気カードも、数年間使用されてきている。このような磁気カードは、オンボードリーダで認識することができ、適切な許可があれば、イグニションシステムおよび／または燃料供給を解除し、自動車両に警報システムがあればそれを働かないようにできる。このような自動車両用ロックシステムについては、たとえば初めに引用したＳＥ　９３００３２９Ａという文献の中で説明されている。

【０００５】ＤＥ　４４０９１６６Ｃ１では、自動車両用の異なるタイプのアクセス制御装置が説明され、この装置は、同様に記憶ユニットに個人データまたは自動車両固有データまたはその両方を符号化された形式で記憶するポータブルチップカードを使用する。しかし、これは実際には自動車両を動作可能に解除することには使用されないが、道ばたの外部固定制御ユニットおよび自動車両自体の車両制御装置により、チップカードを備えた自動車両へのアクセス許可を要求する。固定制御ユニットとやりとりする信号は、長距離で伝送でき、車両制御装置とチップカードの間でやりとりする信号は、短距離で伝送できる。知られているアクセス制御装置では、さらにチップカードに、当初禁じられている領域へのアクセスに対し課金されるときに、支払い額が借り方に付けられるクレジットメモリを備えることができる。

【０００６】

【発明が解決しようとする課題】これらの知られている方法の重大な欠点は、無許可自動車両ユーザが、特に自動車両泥棒が、チップカードを保有しているだけで簡単に自動車両を始動して逃げ去ることができるという点である。

【０００７】それとは対照的に、本発明の目的は、はじめに説明したタイプの方法と、そのために適したデータキャリアと、「正しい」チップカードを使用できる場合であっても自動車両の無許可の使用がほとんどできない対応する車両装置とを提案することである。

【０００８】

【課題を解決するための手段】本発明によれば、この目的は、データキャリアがデータキャリアの所有者に関するユーザ固有の情報を記憶しており、その情報はリーダによって検出され、オンボードプロセッサに供給され、オンボードで記憶されている情報と比較されるということ、比較の結果に応じて、オンボード認識装置によってさらなる個人情報がユーザに要求され、オンボードプロセッサに供給され、許可できるユーザのアイデンティティに関するオンボードで記憶されている情報と比較されるということ、さらに個人データの比較の結果に応じて、自動車両を動作可能に解除することが行われたり、行われなかったりするということで達成される。

【０００９】

【発明の実施の形態】このようにすると、データキャリアを単に保有しているだけ（無許可の場合も含めて）では動作可能に解除することを行うのに充分でなく、無許可な人物には一般には利用できないさらなる個人情報を入力しないと動作可能に解除することを行えないようになる。ただし、さらに、自動車両泥棒の疑いのある人だと取得や偽造が非常に困難な許可された所有者に関するユーザ固有の情報も、データキャリア内にすでに取り込まれている。したがって動作可能に解除することは、ユーザ固有の個人データキャリアがオンボードシステムで受け付けられ、ユーザの個人認識がオンボードシステムに供給された更なる情報に基づいて行われている場合にのみ実行できる。自動車両泥棒の疑いのある人が、オンボードシステムで受け付けられるタイプのデータキャリアを取得した場合でも、データキャリアは、ユーザ固有情報が必要なため、許可された人から盗まれたものだする。しかしこれはそれ自体、泥棒の疑いのある人に役立つものではなく、認識装置からさらに要求されるさらなる個人情報を保有していないことが確認される。

【００１０】特に単純な方法の変形形態では、たとえば現金自動預入支払装置の作動時のクレジットカードの保護と関連して本来知られているように、個人情報を英数字コードの形式、特に一般に許可されたユーザにのみ知られている暗証番号（個人識別番号＝ＰＩＮ）の形式で認識装置に入力する。この目的のためには、オンボード認識装置を経由する英数字入力キーパッドがあるだけでよい。

【００１１】他の方法の変形形態では、建物への出入りと関連してすでに本来知られているように、個人情報をユーザの電子指紋の形式で認識装置に供給する。

【００１２】考えられる他の追加の保護形式として、音響信号を使い認識装置に個人情報を供給するという方法がある。これらの信号は、ユーザ自身が自分の声や、さもなければ音声発生装置を使って発することができる。

【００１３】この方法の変形形態の好ましい他の発展形では、音響信号は、オンボード音声認識装置によって認識されるコードワードを含み、動作可能に解除することを許可する記憶されているコードワードと比較される。この発展形の利点は、キーボードでコードワードを入力する必要がなく、ユーザが単に話すだけでよいという点である。

【００１４】前記方法の変形形態の特に好ましい他の発展形として、音響信号にユーザが発した音声信号が含まれ、オンボード音声認識装置内で、動作可能に解除することを許可する指定されたユーザの音声の記憶されている周波数パターンと比較するものがある。人間の音声信号の周波数パターンは、個人ごとに際だって異なるので、基本的に、個人を識別する「古典的な」指紋による方法よりもなおいっそう適していることが犯罪学から知られている。

【００１５】有用な方法の変形形態では、個人情報を光信号の形式で認識装置に供給する。前記音響信号の場合のように、同様に光信号はユーザが直接発したり、追加の装置（ランプなど）を使って発することができ、その場合、認識装置には光検出器が装備されていなければならない。

【００１６】この方法の変形形態の有用な他の発展形として、光信号が特定の周波数またはパルス列またはその両方の光を含み、動作可能に解除することを許可する記憶されている周波数またはパルス列またはその両方と、オンボードで比較するというものがある。このような個別化された周波数またはパルス列またはその両方は、ミニレーザなどの知られている照射手段で容易に実現できる。

【００１７】前記方法の変形形態の好ましい他の発展形として、光信号がイメージパターンを含み、オンボードイメージ認識装置で、動作可能に解除することを許可する記憶されているイメージパターンと比較するというものがある。このようなイメージパターンもまた、高度に個人化することができ、したがってユーザ固有のものである。

【００１８】前記方法の変形形態の単純な他の発展形では、イメージパターンを、たとえば許可されたユーザが帯びている認識バッジに加えることができる。

【００１９】ただし、特に好ましい他の発展形として、イメージパターンに当該ユーザの顔、特にユーザの写真だけでなくユーザの実際の現在の容貌を含むものがある。個人イメージ認識装置は、許可されたユーザの様々な顔のイメージパターンと、瞬間的に提示されたイメージパターンとを比較できなければならない。このような形およびパターンの認識プログラムは、それ自体すでに知られている。

【００２０】個人許可を要求する他の方法として可能なものに、特定のユーザの体重信号を使い認識装置に個人情報を供給し、体重信号を、オンボードで記憶されている許可されたユーザの体重値と比較するという方法がある。これは、たとえば運転者の座席に組み込んだ体重センサを使って比較的容易に測定できるが、もちろん、体重情報が妥当な制限範囲内で個々のユーザに関係している必要がある。とにかくすでにユーザ固有の情報によって個別化されている、データキャリアを取得した自動車両泥棒の疑いのある人がさらに、許可されているユーザの正しい「体重範囲」を有することはまずあり得ない。

【００２１】特に好ましい方法の変形形態として、許可できるユーザのアイデンティティに関するオンボードで記憶されている情報を、マスタコードで変更できるというものがある。この方法では、たとえば、レンタカー会社（car hire firm）やタクシー会社（company vehicle fleet）で、データキャリアを常時移り変わりのある許可されたユーザのグループに適応させることができる。

【００２２】他の特に有用な方法の変形形態として、オンボードプロセッサが、好ましくは特定のユーザが追加コマンドを入力した結果により、少なくとも１つの個人電子日誌を付けるというものがある。また電子日誌は基本的に、全ユーザについて、車両を使用するごとに、自動的にかつ強制的に付けることができ、これもまた、たとえば常時移り変わりのある運転手が自動車両を運転する大きなタクシー会社や自動車両共有の変形形態に適している。データキャリア上のユーザ固有の情報および認識装置に供給される追加個人情報を利用することにより、潜在的に可能なすべての運転者に対して、全車両において自動的に個々の電子日誌を付けることができる。

【００２３】さらにこの電子日誌を公務の目的に適ったものにするために、この実施形態の他の発展形では、マスタコードが知られている場合でも後で操作できないように、電子日誌のデータを書込み保護付きでオンボードで記憶するものとする。したがって、電子日誌は、たとえば証拠書類、場合によっては法律上の証拠とするため警察の調査、金融調査、税務調査などにも有用である。

【００２４】特に好ましい他の方法の変形形態では、データキャリアに記憶されているユーザ固有の情報に、所有者に関する公式データを入れる、特に所有者の運転免許に関するデータを入れる。長期間検討したこの方法では、自動車両の運転を運転免許の有効性に直接結びつけることができ、またデータキャリアに記憶されている更なる自動車両または保有者またはその両方に固有のデータにより、自動車両の運転許可に直接結びつけることができる。したがって、たとえばスモッグ警報による公式の運転禁止、運転免許保有者による個人的違反行為、または運転免許制限（たとえば、保有者が夜盲症の場合）も、直接に、コストのかかる警察の検査を利用することなく実施できる。

【００２５】他の方法の変形形態では、データキャリアに記憶されているユーザ固有の情報に、保険会社のデータ、特に所有者の第三者保険に関するデータを入れる。このようにすると、たとえば不適切な第三者保険に入っている自動車両をまったく運転できないようにし、保険に入っていない人が事故を起こした場合に、損害請求を強制できないような状況に一般大衆が陥らないよう保護することが可能である。

【００２６】さらに、本発明による方法の変形形態では、データキャリアに記憶されているユーザ固有の情報に、金融機関のデータ、特に所有者の勘定残高または信用等級に関するデータを入れることができる。このため、たとえば「電子イグニションキー」として使用される本発明に基づくチップカードに、クレジットカード機能を付加できる可能性も広がる。

【００２７】データ保護のため、さらに、許可されている所有者を保護するために、所有者のデータキャリア上の公式データ、保険会社データ、金融機関データ、他の機関のデータの入力または変更ができるのは、特定の機関の許可されている代理人だけである。

【００２８】特に好ましい他の発展形として、特定の機関の適当な機器を用いて、所有者のデータキャリア上の公式データ、保険会社データ、および金融機関データを、自動的に変更するものがある。これは、この目的のために用意されている装置内のチップカードの専用処理（たとえば、クレジットカード機能のクレジットの「ロード」や、道路交通法および規制を守らなかった場合に運転免許罰則点数の入力または抹消、チップカードへの保険担保の入力）により、またはさらに、たとえばロック機能がチップカードに組み込まれている場合に、一定時間間隔が経過したときに自動的に、実行させることができる。

【００２９】本発明に基づく他の特に好ましい方法の変形形態として、ユーザのデータキャリアから送られる、あるいはオンボード認識装置を介して送られる、あるいはその両方の情報のオンボード評価を、データバンク問合せで、特に無線によって行うものがある。この方法では、要求機能と評価機能は、実際のデータ処理を自動車両自体から取り除いており、かなり広い基準をもとにするため、自動車両にそれほどの処理および記憶容量を持たせる必要はない。

【００３０】他の特に好ましい方法の変形形態では、解除される自動車両の運転者を識別するユーザ固有の情報の少なくとも一部は、外部装置、たとえば警察の速度検査地点、国境管理地点、駐車場またはホテルまたは修理工場などのサービス提供者のアクセス装置、現金自動預入支払装置などへ、たとえば無線によって転送されるものとしている。これにより、個々の機能を考慮しながらも、大規模で広い範囲にわたる自動車両の運転と関連するサービスおよび制御機能を自動処理することが可能になる。

【００３１】特定のユーザの個人プリセットパラメータにより、ユーザ固有の情報が、座席、ステアリングホイール、ミラーなどの自動車両要素を個々に調整するために使用される他の方法の変形形態では、快適さと使いやすさが向上する。したがって、各ユーザは、自分のデータキャリアに自分にとってもっとも快適だと思う設定パラメータを、たとえばマスタコードを使用することによって個々に記憶させることができる。問題の自動車両を使用するときに、これらの設定パラメータは、エンジンを始動する前に、座席、ステアリングホイール、ミラーの電気的な調整により自動的に実施される。

【００３２】本発明による他の有用な方法の変形形態として、認識装置またはプロセッサ中での個人データ比較結果が、連続して数回否定的であった場合、警報が発せられるものがある。この機能は、たとえば、ＰＩＮの入力が何回か成功しなかったときに、現金自動預入支払装置によってカードが保持されるバンクカードの例で知ら

れている。

【００３３】さらに、本発明の範囲には、本発明に基づく前記方法ステップを実行するためのユーザ固有の情報を格納する記憶手段を備える自動車両を動作可能に解除することに使用されるデータキャリア、特にチップカードも含まれる。

【００３４】さらに、本発明の範囲には、本発明に基づく前記方法ステップを実行するための手段を備える車両装置も含まれる。

【００３５】本発明に基づく車両装置の特に好ましい実施形態として、ユーザのデータキャリアからユーザ固有

の情報を検出するリーダに、さらなる個人情報を要求するオンボード認識装置を備えるものがある。たとえば、リーダに、ＰＩＮの英数字入力用のキーパッドを装備することができる。

【００３６】オンボードプロセッサが、無線インタフェースを介して外部データ処理システムに接続される実施形態も、特に有用である。この方法により、自動車両の処理容量および記憶容量を、本発明に基づく方法を応用することによって実現される（ほとんど無制限の）可能性を制限することなく、きわめて小さくすることができる。

フロントページの続き

(51) Int. Cl.[7]		識別記号	F I		テーマコード（参考）
Ｅ０５Ｂ	49/00		Ｅ０５Ｂ 49/00	Ｚ	
	65/12		65/12	Ａ	

【外国語明細書】

1. Title of Invention

A Process for Operationally Releasing a Motor Vehicle and a Chip Card and Vehicle Device Therefore

2. Claims

1. A process for operationally releasing a motor vehicle, for example by releasing the ignition system and/or fuel supply and/or disabling an alarm system of the motor vehicle, wherein the operational release takes place as a result of the supply of a data carrier, in particular a chip card, into an on-board reader, when the reader recognises that the supplied data carrier is valid and has stored data authorising the release, characterised in that the data carrier has stored user-specific information relating to the owner of the data carrier, which information is detected by the reader, supplied to an on-board processor, and compared therein with information stored on-board, that as a function of the result of the comparison, further personal information is requested of the user by an on-board recognition device, supplied to the on-board processor and compared with information stored on-board relating to the identity of the permissible user(s), and that as a function of the result of the personal data comparison the operational release of the motor vehicle does or does not take place.

2. A process according to Claim 1, characterised in that the personal information is input into the recognition device in the form of an alphanumerical code, in particular a secret number generally known only to the authorised users (personal identification number = PIN).

3. A process according to one of the preceding claims, characterised in that the personal information is supplied to the recognition device in the form of an electronic fingerprint of the user.

4. A process according to one of the preceding claims, characterised in that the personal information is supplied to the recognition device by means of acoustic signals.

5. A process according to Claim 4, characterised in that the acoustic signals contain a code which is recognised by an on-board speech recognition device and compared with a stored code word authorising the operational release.

6. A process according to Claim 4 or 5, characterised in that the acoustic signals comprise voice signals emitted by the user and are compared in an on-board speech recognition device with stored frequency patterns of the voices of specific users which authorise the operational release.

7. A process according to one of the preceding claims, characterised in that the personal information is supplied to the recognition device in the form of optical signals.

8. A process according to Claim 7, characterised in that the optical signals comprise light of a specific frequency and/or pulse sequence and are compared on-board with stored frequencies and/or pulse sequences authorising the operational release.

9. A process according to Claim 7 or 8, characterised in that the optical signals comprise image patterns and are compared in an on-board image recognition device with stored image patterns authorising the operational release.

10. A process according to Claim 9, characterised in that the image patterns comprise the face of the particular user.

11. A process according to one of the preceding claims, characterised in that the personal information is supplied to the recognition device by means of weight signals of the

particular user and that the weight signals are compared with weight values, stored on-board, of authorised users.

12. A process according to one of the preceding claims, characterised in that the information stored on-board relating to the identity of the permissible user(s) can be altered by means of a master code.

13. A process according to one of the preceding claims, characterised in that the on-board processor keeps at least one personal electronic log-book, preferably as a result of an additional command to be input by the particular user.

14. A process according to Claim 13, characterised in that the data of the electronic log-book are stored on-board with write-protection such that they cannot be subsequently manipulated even when a master code is known.

15. A process according to one of the preceding claims, characterised in that the user-specific information stored on the data carrier comprises official data relating to the owner, in particular data relating to the driving license of the owner.

16. A process according to one of the preceding claims, characterised in that the user-specific information stored on the data carrier comprises data of insurance companies, in particular data relating to third-party insurance of the owner.

17. A process according to one of the preceding claims, characterised in that the user-specific information stored on the data carrier comprises data of credit institutions, in particular data relating to account balances or credit ratings of the owner.

18. A process according to one of Claims 15 to 17, characterised in that the official data, insurance company data and credit institution data can be entered or altered on the data carrier of the owner only by authorised agents of the particular institution.

19. A process according to Claim 18, characterised in that the official data, insurance company data and credit institution data are altered automatically on the data carrier of the owner by means of suitable devices of the particular institution.

20. A process according to one of the preceding claims, characterised in that the on-board evaluation of the information supplied by the data carrier of the user and/or via the on-board recognition device is performed by making a data bank enquiry, in particular via radio.

21. A process according to one of the preceding claims, characterised in that the user-specific information for identifying the driver of the released motor vehicle is forwarded at least in part, for example via radio, to external devices, for example police speed check points, border control points, access devices to car parks, hotels or repair workshops, automatic teller machines and the like.

22. A process according to one of the preceding claims, characterised in that the user-specific information is used to individually adjust vehicle elements such as seat, steering wheel, mirror etc. in accordance with personalized, preset parameters of the particular user.

23. A process according to one of the preceding claims, characterised in that an alarm is given if the result of the personal data comparison in the recognition device or processor is negative several times in succession.

24. A data carrier, in particular a chip card, for operationally releasing a motor vehicle with storage means containing user-specific information for the implementation of the process steps of one or more processes according to Claims 1 to 23.

25. A vehicle device with means for implementing the process steps of one or more processes according to Claims 1 to 23.

26. A vehicle device according to Claim 25, characterised in that the reader for detecting the user-specific information from the data carrier of the user comprises the on-board recognition device for requesting further personal information.

27. A vehicle device according to Claim 25 or 26, characterised in that the on-board processor is connected via a radio interface to an external data processing system.

3. Detailed Description of Invention

The invention relates to a process for operationally releasing a motor vehicle, for example by releasing the ignition system and/or fuel supply and/or disabling an alarm system of the motor vehicle, wherein the operational release takes place as a result of the supply of a data carrier, in particular a chip card, into an on-board reader, when the reader recognises that the supplied data carrier is valid and has stored data authorising the release, and the invention relates to a suitable data carrier and corresponding vehicle devices therefore.

Such a process is known from SE 93 00 329 A.

A number of technical devices are commercially available for protecting motor vehicles from unauthorised use, in particular from theft. In addition to lockable vehicle doors, which have been used since the beginning of automobile construction, for many decades an ignition lock has been in use which can generally be released by means of an ignition key which normally simultaneously serves to open the vehicle doors.

As such mechanical locks can easily be "cracked" by thieves with technical know-how, for increased theft protection magnetic cards with built-in electronic chips have also been in use for some years; such magnetic cards can be recognised by an on-board reader and, in the case of appropriate authorization, can release the ignition system and/or fuel supply and disable possible alarm systems in the motor vehicle. Such a locking system for motor vehicles is described for example in the document SE 93 00 329 A referred to in the introduction.

DE 44 09 166 C1 describes a different type of access control device for a vehicle which likewise uses a portable chip card whose storage unit stores personal and/or vehicle-specific data in coded form. However this does not serve actually to operationally release the vehicle but requests access authorization to the vehicle provided with the chip card via an external, stationary control unit at the roadside and via a vehicle control device in the vehicle itself. The signals to and from the stationary control unit can be transmitted over a long range and the signals between the vehicle control device and the chip card can be transmitted over a short range. In the known access control device the chip card can also comprise a credit memory from which a payment amount is debited when access to the initially barred area is subject to charge.

An essential shortcoming of these known approaches consists in that an unauthorised vehicle user, in particular also a vehicle thief, can easily start up and drive away the vehicle simply by being in possession of the chip card.

In contrast, the object of the present invention is to propose a process of the type described in the introduction and a data carrier suitable therefore and corresponding vehicle device which virtually eliminate the unauthorised use of the motor vehicle even when the "correct" chip card is available.

In accordance with the invention, this object is achieved in that the data carrier has stored user-specific information relating to the owner of the data carrier, which information is detected by the reader, supplied to an on-board processor and compared therein with information stored on-board, that as a function of the result of the

comparison, further personal information is requested of the user by an on-board recognition device, supplied to the on-board processor, and compared with information stored on-board relating to the identity of the permissible user(s), and that as a function of the result of the personal data comparison, the operational release of the motor vehicle does or does not take place.

In this way it is ensured that not just the mere (possibly unauthorised) possession of the data carrier is sufficient to facilitate the operational release, but only the input of further personal information generally unavailable to an unauthorised person. Additionally however, user-specific information relating to the authorised owner, which a potential vehicle thief could obtain or forge only with great difficulty, is also already contained on the data carrier. The operational release can thus only take place both if the user-specific, personalized data carrier is accepted by the on-board system and if a personal recognition of the user has taken place on the basis of further information supplied to the on-board system. Even if a potential vehicle thief has obtained a data carrier of a type which would be accepted by the on-board system, the data carrier would have had to have been stolen from an authorised person due to the requirement of the user-specific information. This in itself would be of no further help to the potential thief however, as he will certainly not be in possession of the further personal information additionally requested by the recognition device.

In a particularly simple process variant, the personal information is input into the recognition device in the form of an alphanumerical code, in particular a secret number generally known only to the authorised users

(personal identification number = PIN), for example as known per se in connection with the protection of credit cards in the operation of automatic teller machines. For this purpose only an alphanumerical input keypad is required by way of on-board recognition device.

In another process variant, the personal information is supplied to the recognition device in the form of an electronic fingerprint of the user, as already known per se in connection with buildings access.

Another possible form of additional protection consists in supplying personal information to the recognition device by means of acoustic signals. These can either be emitted by the user himself by the use of his voice or however by means of a sound-generating device.

In a preferred further development of this process variant, the acoustic signals contain a code word which is recognised by an on-board speech recognition device and compared with a stored code word which authorises the operational release. The advantage of this further development consists in that the code word need not be input via a keyboard but is simply spoken by the user.

A particularly preferred further development of the above process variant consists in that the acoustic signals comprise voice signals emitted by the user and are compared in an on-board speech recognition device with stored frequency patterns of the voices of specified users which authorise the operational release. It is known from criminology that the frequency patterns of human voice signals are so markedly personalized that basically they are even more suitable than "classic" fingerprints for identifying an individual.

In another advantageous process variant the personal information is supplied to the recognition device in the form of optical signals. Like the acoustic signals described in the foregoing, the optical signals can likewise be emitted directly from the user or by the use of an additional device (lamp etc.), in which case the recognition device must comprise an optical detector.

An advantageous further development of this process variant consists in that the optical signals comprise light of a specific frequency and/or pulse sequence and are compared on-board with stored frequencies and/or pulse sequences which authorise the operational release. Such individualized frequencies and/or pulse sequences can readily be implemented in known illumination means, such as mini-lasers.

A preferred further development of the above described process variant is that in which the optical signals comprise image patterns and are compared in an on-board image recognition device with stored image patterns which authorise the operational release. Such image patterns can again be highly personalized and thus user-specific.

In simple further developments of the above process variant, the image patterns can be applied for example to an identification badge carried by the authorised user.

However, a particularly preferred further development is that in which the image patterns comprise the face of the relevant user, in particular not merely a photograph of the user but his actual current appearance. The personal image recognition device must then be capable of comparing image patterns of the faces of different authorised users with an

instantaneously presented image pattern. Such shape- and pattern recognition programs are already known per se.

Another possibility of requesting a personal authorization consists in that the personal information is supplied to the recognition device by means of weight signals of the particular user and that the weight signals are compared with weight values of authorised users stored on-board. This can be determined relatively easily by means of a weight sensor built-in for example to the driver's seat, it being necessary of course that the weight information relates to the individual user within reasonable limits. It is rather unlikely that a potential vehicle thief who has obtained the data carrier, anyhow already individualised by the user-specific information, will also possess the correct "weight category" of the authorised user.

A particularly preferred process variant is that in which the information stored on-board relating to the identity of the permissible user(s) can be altered by means of a master code. In this way for example a car hire firm or company vehicle fleet can adapt the data carriers to the constantly changing group of authorised users.

Another particularly advantageous process variant is that in which the on-board processor keeps at least one personal electronic log-book, preferably as a result of an additional command to be input by the particular user. The electronic log-book can also basically be kept automatically and compulsorily for all users and in the case of each use of the vehicle, which again is suitable for example for a large company vehicle fleet or car-sharing variants where the vehicles are operated by constantly changing drivers. By means of the user-specific

information on the data carrier and the additional personal information supplied to the recognition device, an individual electronic log-book can be kept automatically in every vehicle, potentially for every possible driver.

In order also to render the electronic log-book suitable for official purposes, in a further development of this embodiment it is provided that the data of the electronic log-book are stored on-board with write-protection, such that even when a master code is known they cannot be subsequently manipulated. As a result, the electronic log-book is also useful for example in the case of police enquiries, financial checks, tax checks and the like by way of documentary evidence and possibly even legal evidence.

In another particularly preferred process variant, the user-specific information stored on the data carrier comprises official data relating to the owner, in particular data relating to the driving license of the owner. In this way, considered over the long-term, the operation of a motor vehicle can be directly linked to the validity of a driving license and, via further vehicle- and/or holder-specific data stored on the data carrier, also to the operating permission of the vehicle. Thus official driving bans, for example due to a smog alert, personal offenses by the holder of a driving license, or driving license restrictions (e.g. in the event of the night-blindness of the holder) can also be enforced directly and without the costly use of police checks.

In other process variants, the user-specific information stored on the data carrier comprises data of insurance companies, in particular data relating to third-party insurance of the owner. In this way it is possible for example to prevent a vehicle with inadequate third party

insurance from being operated at all, which protects the general public from the situation in which claims for damages may be unenforceable in the case of accidents caused by uninsured persons.

Furthermore, in a variant of the process according to the invention the user-specific information stored on the data carrier can comprise data of credit institutions, in particular data relating to account balances or credit-ratings of the owner. This opens up the possibility of also impressing credit card functions for example on the chip card which, in accordance with the invention, serves as "electronic ignition key".

For reasons of data protection and also to protect the authorised owner, the official data, insurance company data, credit institution data, or data of other institutions are to be capable of being entered or altered on the data carrier of the owner only by authorised agents of the particular institution.

A particularly preferred further development is that in which the official data, insurance company data, and credit institution data are altered automatically on the data carrier of the owner by means of suitable equipment of the particular institution. This can be effected either by special processing of the chip card in a device provided for this purpose (for example "loading" credit for the credit card function, entering or erasing driving license penalty points in the case of non-compliance with road-traffic laws and regulations, or entering insurance cover on the chip card) or also automatically for example as a result of the elapse of a time interval if a lock function is integrated on the chip card.

Another particularly preferred variant of the process according to the invention is that in which the on-board evaluation of the information supplied by the data carrier of the user and/or via the on-board recognition device is performed by making a data bank enquiry, in particular via radio. In this way the request- and evaluation function can be placed on a considerably broader basis since the actual data processing is removed from the vehicle itself so that it is unnecessary to provide substantial processing- and storage capacity in the vehicle.

In another particularly preferred process variant it is provided that the user-specific information identifying the driver of the released vehicle is forwarded at least in part, for example via radio, to external devices, for example to police speed check points, to border control points, to access equipment of service providers such as car parks, hotels or repair workshops, to automatic teller machines and the like. This renders possible the automatic handling of services and control functions in association with the operation of a motor vehicle on a large scale and to a wide extent while still taking into account individual features.

Increased comfort and user-friendliness is provided by a further process variant in which the user-specific information is used to individually adjust vehicle elements such as seat, steering wheel, mirror etc. in accordance with personalized preset parameters of the particular user. Thus each user can individually store on his data carrier the setting parameters which are most comfortable for him, for example by the use of a master code; when the vehicle in question is used, these setting parameters are then automatically implemented by means of electrical seat-, steering wheel- and mirror adjustment before the engine is

started.

Another advantageous variant of the process according to the invention is that in which an alarm is given if the result of the personal data comparison in the recognition device or processor is negative several times in succession. This feature is known for example in the context of bank cards where, after several unsuccessful inputs of a PIN, the card is retained by an automatic teller machine.

The scope of the present invention also includes a data carrier, in particular a chip card, for the operational release of a motor vehicle with storage means containing user-specific information for the implementation of the above described process steps according to the invention.

The scope of the invention also includes a vehicle device equipped with means for implementing the above described process steps according to the invention.

A particularly preferred embodiment of the vehicle device according to the invention is that in which the reader for detecting the user-specific information from the data carrier of the user comprises the on-board recognition device for requesting further personal information. For example the reader can be equipped with a keyboard for the alphanumerical input of a PIN.

An embodiment in which the on-board processor is connected via a radio interface to an external data processing system is also particularly advantageous. In this way the processing and storage capacity within the motor vehicle can be kept extremely small without restricting the (virtually unlimited) possibilities offered by the application of the process according to the invention.

1. Abstract

A process for operationally releasing a motor vehicle by supplying a data carrier into an on-board reader is characterised in that the data carrier has stored user-specific information relating to the owner, which information is detected by the reader, supplied to an on-board processor, and compared with information stored therein, that further personal information is requested of the user by an on-board recognition device, supplied to the processor, and compared with information stored on-board relating to the identity of the permissible user(s), and that as a function of the result of the personal data comparison, the motor vehicle is operationally released. In this way it is possible virtually to eliminate the unauthorised use of the motor vehicle, even when the "correct" chip card is available.